

THE MERIT FACTOR OF BINARY ARRAYS DERIVED FROM THE QUADRATIC CHARACTER

KAI-UWE SCHMIDT

ABSTRACT. We calculate the asymptotic merit factor, under all cyclic rotations of rows and columns, of two families of binary two-dimensional arrays derived from the quadratic character. The arrays in these families have size $p \times q$, where p and q are not necessarily distinct odd primes, and can be considered as two-dimensional generalisations of a Legendre sequence. The asymptotic values of the merit factor of the two families are generally different, although the maximum asymptotic merit factor, taken over all cyclic rotations of rows and columns, equals $36/13$ for both families. These are the first non-trivial theoretical results for the asymptotic merit factor of families of truly two-dimensional binary arrays.

1. INTRODUCTION

We consider an *array of size* $n \times m$ to be an infinite matrix $A = (a_{ij})$ of real-valued elements satisfying

$$a_{ij} = 0 \quad \text{unless } 0 \leq i < n \text{ and } 0 \leq j < m.$$

The array is called *binary* if a_{ij} takes values only in $\{1, -1\}$ for all i, j satisfying $0 \leq i < n$ and $0 \leq j < m$, and is called *ternary* if a_{ij} takes values only in $\{0, 1, -1\}$. Given integers u and v , the *aperiodic autocorrelation* of $A = (a_{ij})$ at displacement (u, v) is defined to be

$$C_A(u, v) := \sum_{i,j} a_{ij} a_{i+u, j+v}.$$

We refer to an array of size $n \times 1$ as a *sequence of length* n , abbreviating the array (a_{i0}) to (a_i) and the aperiodic autocorrelation $C_A(u, 0)$ to $C_A(u)$.

Binary arrays with small out-of-phase aperiodic autocorrelation have a wide range of applications in digital communications and storage systems, including radar [1] and steganography [23]. Ideally, we would like to find a binary array A of size $n \times m$ satisfying

$$(1) \quad |C_A(u, v)| \leq 1 \quad \text{for all } (u, v) \neq (0, 0),$$

in which case, A is called a *Barker array* [1]. However, it was recently shown by Davis, Jedwab, and Smith [6] that a (truly two-dimensional) Barker array must have size 2×2 . (Barker sequences of length n , namely $n \times 1$ Barker arrays, are known for $n \in \{2, 3, 4, 5, 7, 11, 13\}$, and any other Barker sequence must have even length [22] greater than 10^{29} [18].)

Date: 30 June 2010 (revised 18 July 2011).

2010 *Mathematics Subject Classification.* Primary: 94A55; Secondary: 68P30, 05B10.

The author is supported by Deutsche Forschungsgemeinschaft (German Research Foundation) under Research Fellowship SCHM 2609/1-1.

Since the Barker array criterion (1) is too restrictive for array dimensions exceeding 2×2 , it is natural to define a measure for the collective smallness of the aperiodic autocorrelation values of a binary array. One such measure is the *merit factor*, which is defined for a binary array $A = (a_{ij})$ of size $n \times m$ with $nm > 1$ to be

$$F(A) := \frac{(nm)^2}{\sum_{(u,v) \neq (0,0)} [C_A(u,v)]^2}.$$

Let $F_{n,m}$ denote the maximum value of $F(A)$ taken over all 2^{nm} binary arrays A of size $n \times m$, and abbreviate $F_{n,1}$ to F_n . We note that the mean of $1/F(A)$, taken over all binary sequences A of length n , equals $1 - 1/n$ [19]. The argument of [19] easily generalises to two dimensions: the mean of $1/F(A)$, taken over all 2^{nm} binary arrays A of size $n \times m$, equals $1 - 1/(nm)$. It follows that $F_{n,m} \geq nm/(nm - 1)$, which asymptotically equals 1 and provides a first benchmark result.

A number of theoretical and computational results on F_n are known (see [11] for a survey). One line of research is to calculate F_n for small values of n . At present, F_n has been calculated for all $n \leq 60$ (see [11, Fig. 1], for example). The largest values of F_n currently known are $F_{13} = \frac{169}{12} \simeq 14.08$ and $F_{11} = \frac{121}{10}$, which are attained by Barker sequences. The computational analysis of F_n quickly becomes infeasible as n grows. Another line of research is therefore to construct particular infinite families of binary sequences of increasing length and to calculate their asymptotic merit factor.

The only non-trivial infinite families of binary sequences for which the asymptotic value of the merit factor is known are Rudin-Shapiro sequences [17], Legendre sequences [9], and m -sequences [14], together with some generalisations of these families [10], [15], [20], [12], [13]. The largest proven asymptotic merit factor of a binary sequence family is 6, which is attained by cyclically rotated Legendre sequences (see Theorem 2.1). There is also considerable numerical evidence, though currently no proof, that an asymptotic merit factor greater than 6.34 can be achieved for a family of binary sequences related to Legendre sequences [4].

Much less is known about the value of $F_{n,m}$ for $n, m > 1$. Eggers [7, Tab. 4.2] computed $F_{n,m}$ for $nm \leq 21$ and found lower bounds on $F_{n,m}$ for $nm \leq 121$. Although the data supplied in [7] are very limited, it is apparent that $F_{n,m}$ tends to be smaller than F_{nm} . The largest value of $F_{n,m}$ for $n, m > 1$ reported in [7] equals $F_{4,4} = \frac{16}{3} \simeq 5.33$. However, an elementary construction technique gives binary arrays with larger merit factor. Given two sequences $A = (a_i)$ and $B = (b_j)$ of length n and m , respectively, we follow [5] in defining the *product array* $A \times B := (a_i b_j)$. A straightforward calculation shows that

$$(2) \quad C_{A \times B}(u, v) = C_A(u) C_B(v),$$

from which we deduce

$$(3) \quad \frac{1}{F(A \times B)} = \left(1 + \frac{1}{F(A)}\right) \left(1 + \frac{1}{F(B)}\right) - 1.$$

Let A and B be Barker sequences of length 13 and 11, respectively. It follows from (3) that $F(A \times A) \simeq 6.80$, $F(A \times B) \simeq 6.27$, and $F(B \times B) \simeq 5.81$. Another consequence of (3) is

$$F_{n,m} \geq \frac{F_n F_m}{F_n + F_m + 1}.$$

Currently, no theoretical results on the asymptotic merit factor of families of binary truly two-dimensional arrays are known. Bömer and Antweiler [2] analysed the merit factor of several binary array families numerically. Among the investigated families, two types of array families related to the quadratic character appeared to have largest merit factor. The arrays in the first family were proposed by Calabro and Wolf [5] and have size $p \times q$, and the arrays in the second family were proposed by Bömer, Antweiler, and Schotten [3] and have size $p \times p$, where p and q are (not necessarily distinct) odd primes. Both families can be considered as two-dimensional generalisations of Legendre sequences. The authors of [2] successively applied three operations, namely rotations of rows and columns, stairlike rotations of rows and columns, and proper decimations, and computed the maximum value of the merit factor for arrays of small sizes taken from these families. They then remarked [2, p. 8] that

“... , for large arrays, the ACF [aperiodic autocorrelation function] merit factors of both classes [the above mentioned array families of square size] appear to tend to 3.”,

and asked for a theoretical explanation of this observation.

In this paper we study the merit factor of two families of binary arrays. The arrays in the first family, called *Legendre arrays*, have size $p \times q$, where p and q are (not necessarily distinct) odd primes, and contain as a special case the arrays proposed by Calabro and Wolf [5]. The arrays in the second family, called *quadratic-residue arrays*, have size $p \times p$, where p is an odd prime, and contain as a special case the arrays proposed by Bömer, Antweiler, and Schotten [3]. We calculate, under certain conditions on the growth rate of p relative to q , the asymptotic merit factor at all rotations of rows and columns for both array families. In particular, we show that for both families the asymptotic merit factor equals $\frac{36}{13} \simeq 2.77$ for an optimal rotation of rows and columns. Although we only maximise the merit factor with respect to the first operation considered in [2], namely rotations of rows and columns, this result does not support the conclusion of [3] quoted above. For all other (non-optimal) rotations of rows and columns, the asymptotic merit factor of quadratic-residue arrays is larger than that of square Legendre arrays.

2. TWO FAMILIES OF BINARY ARRAYS

Given an odd prime p and a positive integer m , let $\text{GF}(p^m)$ be the finite field containing p^m elements. Whenever convenient, we treat integers after reduction modulo p as elements in $\text{GF}(p)$. The *quadratic character of $\text{GF}(p^m)$* is the function $\chi : \text{GF}(p^m) \rightarrow \mathbb{R}$ defined by

$$\chi(a) := \begin{cases} 0 & \text{for } a = 0 \\ -1 & \text{for } a \text{ not a square in } \text{GF}(p^m) \\ +1 & \text{otherwise.} \end{cases}$$

This function is multiplicative:

$$(4) \quad \chi(a)\chi(b) = \chi(ab).$$

If $m = 1$, then $(a|p) := \chi(a)$ is the *Legendre symbol*. A *Legendre sequence* $L = (\ell_i)$ of prime length $p > 2$ is defined by

$$\ell_i := \begin{cases} 1 & \text{for } i = 0 \\ (i|p) & \text{for } 1 \leq i < p. \end{cases}$$

If the initial element in a Legendre sequence is changed to zero, so that

$$\ell_i = (i|p) \quad \text{for } 0 \leq i < p,$$

then we call L a *ternary Legendre sequence*.

In what follows, we present two families of binary arrays, which can be considered as two-dimensional generalisations of Legendre sequences. Let p and q be two (not necessarily distinct) odd primes, and let $\mathcal{V}_{p,q}$ be the set of ternary arrays $V = (v_{ij})$ of size $p \times q$ satisfying

$$|v_{ij}| = \begin{cases} 1 & \text{for } (i = 0 \text{ and } 0 \leq j < q) \text{ or } (j = 0 \text{ and } 0 \leq i < p) \\ 0 & \text{otherwise.} \end{cases}$$

Then $\mathcal{V}_{p,q}$ contains 2^{p+q-1} arrays, each having $p + q - 1$ nonzero elements. Given ternary Legendre sequences L and K of length p and q , respectively, we define a *Legendre array* X of size $p \times q$ to be a binary array of size $p \times q$ that can be written as

$$X = L \times K + V \quad \text{for some } V \in \mathcal{V}_{p,q}.$$

For example, the array $X = (x_{ij})$ of size $p \times q$, given by

$$x_{ij} := \begin{cases} -1 & \text{for } j = 0 \text{ and } 0 \leq i < p \\ +1 & \text{for } i = 0 \text{ and } 1 \leq j < q \\ (i|p)(j|q) & \text{for } 1 \leq i < p \text{ and } 1 \leq j < q, \end{cases}$$

is a Legendre array of size $p \times q$. This particular array was originally defined by Calabro and Wolf [5], and its merit factor properties were investigated numerically in [2]. In the original paper [5] such an array was called a “quadratic-residue array”. We use the term *Legendre array* to distinguish it from our second family of binary arrays.

Let p be an odd prime, let χ be the quadratic character of $\text{GF}(p^2)$, and let $\{\alpha, \alpha'\}$ be a basis for $\text{GF}(p^2)$ over $\text{GF}(p)$. Following Bömer, Antweiler, and Schotten [3], we define a *quadratic-residue array* $Y = (y_{ij})$ of size $p \times p$ to be a binary array of size $p \times p$ satisfying

$$y_{ij} := \begin{cases} +1 \text{ or } -1 & \text{for } i = j = 0 \\ \chi(i\alpha + j\alpha') & \text{for } 0 \leq i, j < p, (i, j) \neq (0, 0). \end{cases}$$

The class of quadratic-residue arrays (y_{ij}) satisfying $y_{00} = +1$ was defined by Bömer, Antweiler, and Schotten [3], and its merit factor properties were investigated numerically in [2]. In our analysis it will be convenient to change the leading element in a quadratic-residue array to zero. Accordingly, we define the *ternary quadratic-residue array* of size $p \times p$ to be the ternary array $Z = (z_{ij})$ of size $p \times p$ given by

$$(5) \quad z_{ij} := \chi(i\alpha + j\alpha') \quad \text{for } 0 \leq i, j < p.$$

Next we define an operation acting on an array to produce a new array of the same size. Given an array $A = (a_{ij})$ of size $n \times m$ and real numbers s and t , the *rotation* $A_{s,t}$ is the array $B = (b_{ij})$ of size $n \times m$ given by

$$(6) \quad b_{ij} = a_{(i+\lfloor ns \rfloor) \bmod n, (j+\lfloor mt \rfloor) \bmod m} \quad \text{for } 0 \leq i < n \text{ and } 0 \leq j < m.$$

If A is a sequence of length n , we abbreviate $A_{s,0}$ to A_s .

The asymptotic merit factor of a Legendre sequence was calculated for all rotations by Høholdt and Jensen [9].

Theorem 2.1 (Høholdt and Jensen [9]). *Let L be the Legendre sequence of prime length $p > 2$, and let s be a real number satisfying $-\frac{1}{2} < s \leq \frac{1}{2}$. Then*

$$\lim_{p \rightarrow \infty} \frac{1}{F(L_s)} = \frac{1}{6} + 8 \left(|s| - \frac{1}{4} \right)^2.$$

The constraint $-\frac{1}{2} < s \leq \frac{1}{2}$ in Theorem 2.1 is for notational convenience only since by definition A_s is the same as A_{s+1} for every sequence A and all real s . The maximum asymptotic merit factor of a rotated Legendre sequence L_s is 6, which occurs for $s = \pm \frac{1}{4}$.

3. CALCULATION OF THE MERIT FACTOR OF AN ARRAY

Given a positive integer n , let

$$\zeta_n := e^{\sqrt{-1}\pi/n}$$

be a primitive $(2n)$ th root of unity. Let $A = (a_{ij})$ be an array of size $n \times m$. The *generating function* of A is defined to be the power series

$$A(x, y) := \sum_{i,j} a_{ij} x^i y^j.$$

If A is a sequence of length n , we write $A(x)$ for $A(x, y)$.

The next lemma shows how the merit factor of A can be computed from the values $A(\zeta_n^i, \zeta_m^j)$. This approach generalises to two dimensions the method of Høholdt and Jensen [9] to compute the asymptotic merit factor of a sequence.

Lemma 3.1. *Let A be an array of size $n \times m$. Then*

$$\sum_{u,v} [C_A(u, v)]^2 = \frac{1}{4nm} \sum_{i=0}^{2n-1} \sum_{j=0}^{2m-1} |A(\zeta_n^i, \zeta_m^j)|^4.$$

Proof. Straightforward manipulation shows that

$$A(x, y)A(x^{-1}, y^{-1}) = \sum_{u,v} C_A(u, v)x^{-u}y^{-v} \quad \text{for } x \neq 0 \text{ and } y \neq 0,$$

and therefore,

$$(7) \quad |A(x, y)|^2 = \sum_{u,v} C_A(u, v)x^{-u}y^{-v} \quad \text{for } |x| = |y| = 1.$$

Using this identity, an elementary calculation gives

$$\begin{aligned} \frac{1}{4nm} \sum_{i=0}^{2n-1} \sum_{j=0}^{2m-1} |A(\zeta_n^i, \zeta_m^j)|^4 &= \frac{1}{4nm} \sum_{i=0}^{2n-1} \sum_{j=0}^{2m-1} |A(\zeta_n^i, \zeta_m^j)|^2 \overline{|A(\zeta_n^i, \zeta_m^j)|^2} \\ &= \sum_{u,v} [C_A(u, v)]^2, \end{aligned}$$

as required. \square

4. THE MERIT FACTOR OF LEGENDRE ARRAYS

In this section we compute the asymptotic merit factor of Legendre arrays for all rotations, subject to certain conditions on the growth rate of the dimensions. We first record a result on the aperiodic autocorrelation of rotated ternary Legendre sequences, which arises as an immediate corollary of [20, Thm. 3].

Proposition 4.1. *Let L be the ternary Legendre sequence of prime length $p > 2$, and let s be a real number satisfying $-\frac{1}{2} < s \leq \frac{1}{2}$. Then, as $p \rightarrow \infty$,*

$$\frac{1}{p^2} \sum_u [C_{L_s}(u)]^2 = \frac{7}{6} + 8 \left(|s| - \frac{1}{4} \right)^2 + O(p^{-1}(\log p)^2).$$

We note that, as explained after [20, Thm. 3], we can recover Theorem 2.1 from Proposition 4.1. We also need the following bound for the magnitude of a polynomial over \mathbb{C} at a $(2d)$ th root of unity, in terms of its magnitudes at d th roots of unity.

Lemma 4.2. *Let $d > 1$ be odd, and let $A \in \mathbb{C}[x]$ have degree at most $d - 1$. Then*

$$|A(\zeta_d^j)| \leq (2 \log d) \max_{0 \leq k < d} |A(\zeta_d^{2k})| \quad \text{for integer } j.$$

Proof. The bound is trivial in the case that j is even. We may therefore take j to be odd, writing $j = 2\ell + d$ for some integer ℓ so that $\zeta_d^j = -\zeta_d^{2\ell}$. It is then sufficient to bound $|A(-\zeta_d^{2\ell})|$. Now by Lagrange interpolation we have

$$A(x) = \frac{1}{d} \sum_{k=0}^{d-1} \frac{x^d - 1}{x - \zeta_d^{2k}} \zeta_d^{2k} A(\zeta_d^{2k}),$$

and so, since d is odd,

$$\begin{aligned} |A(-\zeta_d^{2\ell})| &\leq \frac{1}{d} \sum_{k=0}^{d-1} \frac{2}{|\zeta_d^{2\ell} + \zeta_d^{2k}|} |A(\zeta_d^{2k})| \\ &\leq \frac{2}{d} \max_{0 \leq k < d} |A(\zeta_d^{2k})| \sum_{m=0}^{d-1} \frac{1}{|1 + \zeta_d^{2m}|}. \end{aligned}$$

The result follows from the inequality $\sum_{m=0}^{d-1} 1/|1 + \zeta_d^{2m}| \leq d \log d$ (which holds since d is odd, see [15, p. 625], for example). \square

The next theorem gives, under certain conditions on the growth rate of p relative to q , the asymptotic merit factor of all 2^{p+q-1} Legendre arrays of size $p \times q$ for all rotations.

Theorem 4.3. *Let \mathcal{N} be an infinite set of products of two not necessarily distinct odd primes, and let N take values only in \mathcal{N} . Write $N = pq$ for odd primes p and q , and suppose that*

$$(8) \quad \frac{q}{p^2} \rightarrow 0 \quad \text{and} \quad \frac{p}{q^2} \rightarrow 0 \quad \text{as } N \rightarrow \infty.$$

Let X be a Legendre array of size $p \times q$, and let s and t be real numbers satisfying $-\frac{1}{2} < s, t \leq \frac{1}{2}$. Then

$$(9) \quad \frac{1}{\lim_{N \rightarrow \infty} F(X_{s,t})} = \left[\frac{7}{6} + 8 \left(|s| - \frac{1}{4} \right)^2 \right] \left[\frac{7}{6} + 8 \left(|t| - \frac{1}{4} \right)^2 \right] - 1.$$

Proof. Let L and K be the ternary Legendre sequences of length p and q , respectively, and write $T := L \times K$. Notice that $T_{s,t} = L_s \times K_t$ and $T_{s,t}(x, y) = L_s(x)K_t(y)$. Then from (2)

$$\sum_{u,v} [C_{T_{s,t}}(u, v)]^2 = \sum_u [C_{L_s}(u)]^2 \cdot \sum_v [C_{K_t}(v)]^2.$$

The condition (8) implies that p and q grow without bound as $N \rightarrow \infty$. We can therefore apply Proposition 4.1 to give

$$(10) \quad \frac{1}{(pq)^2} \sum_{u,v} [C_{T_{s,t}}(u, v)]^2 = \left[\frac{7}{6} + 8 \left(|s| - \frac{1}{4} \right)^2 \right] \left[\frac{7}{6} + 8 \left(|t| - \frac{1}{4} \right)^2 \right] + o(1) \quad \text{as } N \rightarrow \infty.$$

Define

$$(11) \quad \Delta(N) := \frac{1}{(pq)^2} \left| \sum_{u,v} [C_{X_{s,t}}(u, v)]^2 - \sum_{u,v} [C_{T_{s,t}}(u, v)]^2 \right|.$$

We claim that

$$(12) \quad \Delta(N) \rightarrow 0 \quad \text{as } N \rightarrow \infty.$$

The theorem then follows from (10) and (11) and the fact $C_{X_{s,t}}(0, 0) = pq$.

It remains to prove the claim (12). By the definition of a Legendre array, there exists an array $V \in \mathcal{V}_{p,q}$ such that $X_{s,t} = T_{s,t} + V_{s,t}$. From Lemma 3.1 we then have

$$(13) \quad \begin{aligned} \Delta(N) &= \frac{1}{4(pq)^3} \left| \sum_{i=0}^{2p-1} \sum_{j=0}^{2q-1} |T_{s,t}(\zeta_p^i, \zeta_q^j) + V_{s,t}(\zeta_p^i, \zeta_q^j)|^4 - \sum_{i=0}^{2p-1} \sum_{j=0}^{2q-1} |T_{s,t}(\zeta_p^i, \zeta_q^j)|^4 \right| \\ &\leq \frac{1}{4(pq)^3} \sum_{i=0}^{2p-1} \sum_{j=0}^{2q-1} \left| |T_{s,t}(\zeta_p^i, \zeta_q^j) + V_{s,t}(\zeta_p^i, \zeta_q^j)|^4 - |T_{s,t}(\zeta_p^i, \zeta_q^j)|^4 \right|. \end{aligned}$$

Now for $a, b \in \mathbb{C}$ the identity

$$|a + b|^4 = |a|^4 + |b|^4 + 4[\Re(a\bar{b})]^2 + 2|a|^2 \cdot |b|^2 + 4|a|^2 \cdot \Re(a\bar{b}) + 4|b|^2 \cdot \Re(a\bar{b})$$

gives the inequality

$$\left| |a + b|^4 - |a|^4 \right| \leq 4|a|^3 \cdot |b| + 6|a|^2 \cdot |b|^2 + 4|a| \cdot |b|^3 + |b|^4.$$

Apply this bound to (13) to obtain

$$\begin{aligned}
\Delta(N) &\leq \frac{1}{(pq)^3} \sum_{i=0}^{2p-1} \sum_{j=0}^{2q-1} |T_{s,t}(\zeta_p^i, \zeta_q^j)|^3 \cdot |V_{s,t}(\zeta_p^i, \zeta_q^j)| \\
&\quad + \frac{3}{2(pq)^3} \sum_{i=0}^{2p-1} \sum_{j=0}^{2q-1} |T_{s,t}(\zeta_p^i, \zeta_q^j)|^2 \cdot |V_{s,t}(\zeta_p^i, \zeta_q^j)|^2 \\
&\quad + \frac{1}{(pq)^3} \sum_{i=0}^{2p-1} \sum_{j=0}^{2q-1} |T_{s,t}(\zeta_p^i, \zeta_q^j)| \cdot |V_{s,t}(\zeta_p^i, \zeta_q^j)|^3 \\
&\quad + \frac{1}{4(pq)^3} \sum_{i=0}^{2p-1} \sum_{j=0}^{2q-1} |V_{s,t}(\zeta_p^i, \zeta_q^j)|^4.
\end{aligned} \tag{14}$$

Given a ternary Legendre sequence A of length d , it is well known (see [21, p. 182], for example) that $|A(\zeta_d^{2k})| \leq d^{1/2}$ for each integer k . It is easily verified that this implies $|A_r(\zeta_d^{2k})| \leq d^{1/2}$ for each integer k and all real r . Therefore, since $T_{s,t}(x, y) = L_s(x)K_t(y)$, Lemma 4.2 gives

$$|T_{s,t}(\zeta_p^i, \zeta_q^j)| \leq 4(pq)^{1/2} \log(p+q) \quad \text{for all integers } i \text{ and } j.$$

Substitute into (14) to give

$$(15) \quad \Delta(N) \leq 256 \frac{(\log(p+q))^3}{(pq)^{1/2}} S_1 + 96 \frac{(\log(p+q))^2}{pq} S_2 + 16 \frac{\log(p+q)}{(pq)^{3/2}} S_3 + \frac{1}{(pq)^2} S_4,$$

where

$$S_\ell := \frac{1}{4pq} \sum_{i=0}^{2p-1} \sum_{j=0}^{2q-1} |V_{s,t}(\zeta_p^i, \zeta_q^j)|^\ell.$$

From (7) and a straightforward calculation we obtain

$$\begin{aligned}
S_2 &= C_{V_{s,t}}(0, 0) \\
&= p + q - 1.
\end{aligned}$$

The Cauchy–Schwarz inequality gives $S_1 \leq (S_2)^{1/2}$, and since $|V_{s,t}(x, y)| \leq p + q - 1$ for $|x| = |y| = 1$, we also have $S_\ell \leq (p + q - 1)^{\ell-2} S_2$ for $\ell \geq 2$. Substitution into (15) gives

$$\begin{aligned}
\Delta(N) &\leq 256 \left(\frac{p+q-1}{pq} \right)^{1/2} (\log(p+q))^3 + 96 \frac{p+q-1}{pq} (\log(p+q))^2 \\
&\quad + 16 \frac{(p+q-1)^2}{(pq)^{3/2}} \log(p+q) + \frac{(p+q-1)^3}{(pq)^2}.
\end{aligned}$$

Now, using the condition (8), we readily verify our claim (12). \square

There is no loss of generality in Theorem 4.3 from the restriction $-\frac{1}{2} < s, t \leq \frac{1}{2}$ since $A_{s,t}$ is the same as $A_{s+1,t}$ and $A_{s,t+1}$ for every array A and all real s and t . We note that the condition (8) can be relaxed for particular Legendre arrays. For example, let L and K be the Legendre sequences of length p and q , respectively. Then $X = L \times K$ is a Legendre array. From (3) and Theorem 2.1 we conclude that (9) holds under the relaxed condition $p \rightarrow \infty$ and $q \rightarrow \infty$ as $N \rightarrow \infty$.

5. THE MERIT FACTOR OF QUADRATIC-RESIDUE ARRAYS

In this section our goal is to calculate the asymptotic merit factor of a quadratic-residue array of size $p \times p$ at all rotations. We shall assume throughout this section that p is an odd prime. Write the p th roots of unity as

$$\epsilon_j := e^{\sqrt{-1}2\pi j/p} \quad \text{for integer } j.$$

Then, since p is odd, we have

$$\{\zeta_p^i : 0 \leq i < 2p\} = \{\epsilon_j : 0 \leq j < p\} \cup \{-\epsilon_j : 0 \leq j < p\}.$$

Therefore, given an array A of size $p \times p$, Lemma 3.1 asserts that

$$(16) \quad \sum_{u,v} [C_A(u,v)]^2 = \frac{1}{4p^2} \sum_{0 \leq i,j < p} (|A(\epsilon_i, \epsilon_j)|^4 + |A(-\epsilon_i, \epsilon_j)|^4 + |A(\epsilon_i, -\epsilon_j)|^4 + |A(-\epsilon_i, -\epsilon_j)|^4).$$

Our objective is to find an asymptotic expression for the sum on the right-hand side of the identity (16), where A is a rotated ternary quadratic-residue array. Since a ternary quadratic-residue array and a quadratic-residue array differ in only one element, this will be sufficient to compute the asymptotic merit factor of a rotated quadratic-residue array. Before we analyse the sum in (16), we shall need several technical results, which we state in the next subsection.

5.1. Auxiliary Results. The following lemma evaluates the generating function of a ternary quadratic-residue array at p th roots of unity.

Lemma 5.1. *Let χ be the quadratic character of $\text{GF}(p^2)$, and let Z be a ternary quadratic-residue array of size $p \times p$, as defined in (5). Then there exists a basis $\{\beta, \beta'\}$ for $\text{GF}(p^2)$ over $\text{GF}(p)$ such that*

$$Z(\epsilon_k, \epsilon_\ell) = (-1)^{\frac{p+1}{2}} p \chi(k\beta + \ell\beta') \quad \text{for all integers } k, \ell.$$

Proof. Let $\text{Tr} : \text{GF}(p^2) \rightarrow \text{GF}(p)$ be the trace function given by

$$\text{Tr}(x) = x + x^p,$$

and for $b \in \text{GF}(p^2)$, let $\psi_b : \text{GF}(p^2) \rightarrow \mathbb{C}$ be the additive character of $\text{GF}(p^2)$ given by

$$\psi_b(x) := e^{\sqrt{-1}2\pi \text{Tr}(bx)/p}.$$

It is readily verified that

$$(17) \quad \text{Tr}(ax + by) = a \text{Tr}(x) + b \text{Tr}(y) \quad \text{for } a, b \in \text{GF}(p).$$

We choose $\{\beta, \beta'\}$ such that $\{\alpha, \alpha'\}$ (appearing in the definition (5) of Z) and $\{\beta, \beta'\}$ are dual bases, that is,

$$(18) \quad \text{Tr}(\alpha\beta) = 1, \quad \text{Tr}(\alpha\beta') = 0, \quad \text{Tr}(\alpha'\beta) = 0, \quad \text{Tr}(\alpha'\beta') = 1.$$

Such a basis is guaranteed to exist [16, p. 58]. Given integers i, j, k, ℓ , we then have by (17) and (18)

$$\text{Tr}((i\alpha + j\alpha')(k\beta + \ell\beta')) = ik + j\ell,$$

and therefore

$$\begin{aligned}
Z(\epsilon_k, \epsilon_\ell) &= \sum_{0 \leq i, j < p} \chi(i\alpha + j\alpha') e^{\sqrt{-1} 2\pi(i\alpha + j\alpha')/p} \\
&= \sum_{0 \leq i, j < p} \chi(i\alpha + j\alpha') e^{\sqrt{-1} 2\pi \operatorname{Tr}((i\alpha + j\alpha')(k\beta + \ell\beta'))/p} \\
&= \sum_{a \in \operatorname{GF}(p^2)} \chi(a) \psi_{k\beta + \ell\beta'}(a)
\end{aligned}$$

by putting $a := i\alpha + j\alpha'$. The above sum is called a *Gaussian sum*, and it is well known that

$$\sum_{a \in \operatorname{GF}(p^2)} \chi(a) \psi_b(a) = (-1)^{\frac{p+1}{2}} p \chi(b)$$

(see [16, pp. 199–201], for example). This proves the lemma. \square

Our next lemma bounds a certain character sum and evaluates it in special cases.

Lemma 5.2. *Let χ be the quadratic character of $\operatorname{GF}(p^2)$, and define*

$$(19) \quad \Omega(\kappa, \lambda, \mu) := \sum_{x \in \operatorname{GF}(p^2)} \chi(x) \chi(x + \kappa) \chi(x + \lambda) \chi(x + \mu) \quad \text{for } \kappa, \lambda, \mu \in \operatorname{GF}(p^2)$$

and

(20)

$$I := \{(\kappa, \kappa, 0) : \kappa \in \operatorname{GF}(p^2)\} \cup \{(\kappa, 0, \kappa) : \kappa \in \operatorname{GF}(p^2)\} \cup \{(0, \kappa, \kappa) : \kappa \in \operatorname{GF}(p^2)\}.$$

Then

$$(21) \quad \Omega(\kappa, \kappa, 0) = \begin{cases} p^2 - 1 & \text{for } \kappa = 0 \\ p^2 - 2 & \text{for } \kappa \neq 0 \end{cases}$$

and

$$(22) \quad |\Omega(\kappa, \lambda, \mu)| \leq 3p \quad \text{for } (\kappa, \lambda, \mu) \notin I.$$

Proof. Since χ is multiplicative by (4),

$$\begin{aligned}
\Omega(\kappa, \kappa, 0) &= \sum_{x \in \operatorname{GF}(p^2)} [\chi(x(x + \kappa))]^2 \\
&= \sum_{x \in \operatorname{GF}(p^2) \setminus \{0, -\kappa\}} 1
\end{aligned}$$

using $\chi(0) = 0$ and $[\chi(x)]^2 = 1$ for all nonzero $x \in \operatorname{GF}(p^2)$. This proves (21).

To prove (22), we use a special case of a result on multiplicative character sums with polynomial arguments [16, Thm. 5.41], which can be stated as follows. If $f \in \operatorname{GF}(p^2)[x]$ is a monic polynomial of positive degree d that is not a square (that is, $f(x)$ cannot be written as $f(x) = [g(x)]^2$ for some polynomial $g \in \operatorname{GF}(p^2)[x]$), then

$$(23) \quad \left| \sum_{x \in \operatorname{GF}(p^2)} \chi(f(x)) \right| \leq (d - 1)p.$$

For all $(\kappa, \lambda, \mu) \notin I$, the polynomial $f(x) := x(x + \kappa)(x + \lambda)(x + \mu)$ is not a square. Using the multiplicativity (4) of χ , application of (23) gives (22). \square

The following technical lemma can be obtained from the results of [9] and [15].

Lemma 5.3. *Define*

$$(24) \quad \Gamma(k, \ell, m) := \sum_{i=0}^{p-1} \frac{\epsilon_i^2}{(1 + \epsilon_i)(\epsilon_k + \epsilon_i)(\epsilon_\ell + \epsilon_i)(\epsilon_m + \epsilon_i)} \quad \text{for integer } k, \ell, m.$$

Then

$$(25) \quad \Gamma(k, k, 0) = \begin{cases} \frac{p^2(p^2 + 2)}{48} & \text{for } k \equiv 0 \pmod{p} \\ \frac{p^2}{2} \cdot \frac{1}{\epsilon_k |1 - \epsilon_k|^2} & \text{for } k \not\equiv 0 \pmod{p} \end{cases}$$

and

$$(26) \quad \sum_{0 \leq k, \ell, m < p} |\Gamma(k, \ell, m)| \leq (p \log p)^4.$$

Proof. The identity (25) was established in [9, p. 162, Cases 4 and 5]. The bound (26) follows from the inequality $\sum_{i=0}^{p-1} 1/|1 + \epsilon_i| \leq p \log p$ (see [15, p. 625], for example) since

$$\begin{aligned} \sum_{0 \leq k, \ell, m < p} |\Gamma(k, \ell, m)| &\leq \sum_{0 \leq i, k, \ell, m < p} \left| \frac{\epsilon_i^2}{(1 + \epsilon_i)(\epsilon_k + \epsilon_i)(\epsilon_\ell + \epsilon_i)(\epsilon_m + \epsilon_i)} \right| \\ &= \left(\sum_{i=0}^{p-1} \frac{1}{|1 + \epsilon_i|} \right)^4. \end{aligned} \quad \square$$

5.2. Asymptotic Merit Factor Calculation. We are now in a position to analyse asymptotic behaviour of the sum on the right-hand side of the identity (16), where A is a rotated ternary quadratic-residue array. We split the analysis into the following three lemmas.

Lemma 5.4. *Let Z be a ternary quadratic-residue array of size $p \times p$, and let s and t be real numbers satisfying $-\frac{1}{2} < s, t \leq \frac{1}{2}$. Then, as $p \rightarrow \infty$,*

$$\frac{1}{4p^6} \sum_{0 \leq i, j < p} |Z_{s,t}(\epsilon_i, \epsilon_j)|^4 = \frac{1}{4} + O(p^{-2}).$$

Proof. Lemma 5.1 implies

$$|Z(\epsilon_i, \epsilon_j)| = \begin{cases} 0 & \text{for } i \equiv j \equiv 0 \pmod{p} \\ p & \text{otherwise.} \end{cases}$$

Then, using the easily verified identity

$$(27) \quad Z_{s,t}(\epsilon_i, \epsilon_j) = \epsilon_i^{-\lfloor ps \rfloor} \epsilon_j^{-\lfloor pt \rfloor} Z(\epsilon_i, \epsilon_j),$$

we find that

$$\frac{1}{4p^6} \sum_{0 \leq i, j < p} |Z_{s,t}(\epsilon_i, \epsilon_j)|^4 = \frac{1}{4} \left(1 - \frac{1}{p^2} \right),$$

as required. \square

Lemma 5.5. *Let Z be a ternary quadratic-residue array of size $p \times p$, and let s and t be real numbers satisfying $-\frac{1}{2} < s, t \leq \frac{1}{2}$. Then, as $p \rightarrow \infty$,*

$$\begin{aligned} \frac{1}{4p^6} \sum_{0 \leq i, j < p} |Z_{s,t}(-\epsilon_i, \epsilon_j)|^4 &= \frac{1}{3} + 4(|s| - \frac{1}{4})^2 + O(p^{-1}(\log p)^4), \\ \frac{1}{4p^6} \sum_{0 \leq i, j < p} |Z_{s,t}(\epsilon_i, -\epsilon_j)|^4 &= \frac{1}{3} + 4(|t| - \frac{1}{4})^2 + O(p^{-1}(\log p)^4). \end{aligned}$$

Proof. Given an array A , let A^T denote the transpose of A . Since $(Z_{s,t})^T = (Z^T)_{t,s}$ and Z^T is again a ternary quadratic-residue array, it is sufficient to prove the first statement in the lemma.

Let $P \in \mathbb{C}[x]$ be a polynomial of degree $p-1$, and let i and j be integer. We shall make use of the Lagrange interpolation formula

$$(28) \quad P(-\epsilon_i) = \frac{2}{p} \sum_{k=0}^{p-1} P(\epsilon_k) \frac{\epsilon_k}{\epsilon_k + \epsilon_i}$$

(see [9, Eq. (2.5)], for example). It follows that

$$Z_{s,t}(-\epsilon_i, \epsilon_j) = \frac{2}{p} \sum_{k=0}^{p-1} Z_{s,t}(\epsilon_k, \epsilon_j) \frac{\epsilon_k}{\epsilon_k + \epsilon_i}.$$

Set $S := \lfloor ps \rfloor$ and $T := \lfloor pt \rfloor$, and use (27) and Lemma 5.1 to obtain

$$Z_{s,t}(-\epsilon_i, \epsilon_j) = 2(-1)^{\frac{p+1}{2}} \epsilon_j^{-T} \sum_{k=0}^{p-1} \epsilon_k^{-S} \chi(k\beta + j\beta') \frac{\epsilon_k}{\epsilon_k + \epsilon_i},$$

where χ is the quadratic character of $\text{GF}(p^2)$ and $\{\beta, \beta'\}$ is some basis for $\text{GF}(p^2)$ over $\text{GF}(p)$. Since we also have

$$\overline{Z_{s,t}(-\epsilon_i, \epsilon_j)} = 2(-1)^{\frac{p+1}{2}} \epsilon_j^T \sum_{k=0}^{p-1} \epsilon_k^S \chi(k\beta + j\beta') \frac{\epsilon_i}{\epsilon_k + \epsilon_i},$$

we find that

$$\begin{aligned} |Z_{s,t}(-\epsilon_i, \epsilon_j)|^4 &= 16 \sum_{0 \leq a, b, c, d < p} \epsilon_{b-a}^S \epsilon_{d-c}^S \chi(a\beta + j\beta') \chi(b\beta + j\beta') \chi(c\beta + j\beta') \chi(d\beta + j\beta') \\ &\quad \frac{\epsilon_a}{\epsilon_a + \epsilon_i} \frac{\epsilon_i}{\epsilon_b + \epsilon_i} \frac{\epsilon_c}{\epsilon_c + \epsilon_i} \frac{\epsilon_i}{\epsilon_d + \epsilon_i}. \end{aligned}$$

Use the definition (24) of $\Gamma(k, \ell, m)$ to write

$$(29) \quad \sum_{i=0}^{p-1} \frac{\epsilon_a}{\epsilon_a + \epsilon_i} \frac{\epsilon_i}{\epsilon_b + \epsilon_i} \frac{\epsilon_c}{\epsilon_c + \epsilon_i} \frac{\epsilon_i}{\epsilon_d + \epsilon_i} = \epsilon_{c-a} \Gamma(b-a, c-a, d-a),$$

so that after variable relabeling

$$\begin{aligned} \sum_{i=0}^{p-1} |Z_{s,t}(-\epsilon_i, \epsilon_j)|^4 &= 16 \sum_{0 \leq a, k, \ell, m < p} \epsilon_{k-\ell+m}^S \epsilon_\ell \\ &\quad \chi(a\beta + j\beta') \chi(a\beta + j\beta' + k\beta) \chi(a\beta + j\beta' + \ell\beta) \chi(a\beta + j\beta' + m\beta) \Gamma(k, \ell, m). \end{aligned}$$

Put $x := a\beta + j\beta'$ and note that $a\beta + j\beta'$ ranges over $\text{GF}(p^2)$ as a and j range from 0 to $p-1$. By the definition (19) of $\Omega(\kappa, \lambda, \mu)$ we therefore obtain

$$\sum_{0 \leq i, j < p} |Z_{s,t}(-\epsilon_i, \epsilon_j)|^4 = 16 \sum_{0 \leq k, \ell, m < p} \epsilon_{k-\ell+m}^S \epsilon_\ell \Omega(k\beta, \ell\beta, m\beta) \Gamma(k, \ell, m),$$

Let the set I be as defined in (20), and write

$$(30) \quad \frac{1}{4p^6} \sum_{0 \leq i, j < p} |Z_{s,t}(-\epsilon_i, \epsilon_j)|^4 = A + B,$$

where

$$A = \frac{4}{p^6} \sum_{\substack{0 \leq k, \ell, m < p \\ (k\beta, \ell\beta, m\beta) \notin I}} \epsilon_{k-\ell+m}^S \epsilon_\ell \Omega(k\beta, \ell\beta, m\beta) \Gamma(k, \ell, m)$$

$$B = \frac{4}{p^6} \sum_{\substack{0 \leq k, \ell, m < p \\ (k\beta, \ell\beta, m\beta) \in I}} \epsilon_{k-\ell+m}^S \epsilon_\ell \Omega(k\beta, \ell\beta, m\beta) \Gamma(k, \ell, m).$$

Using (22), the sum A can be bounded as

$$|A| \leq \frac{12}{p^5} \sum_{0 \leq k, \ell, m < p} |\Gamma(k, \ell, m)|$$

$$\leq 12 p^{-1} (\log p)^4$$

by (26). Therefore,

$$(31) \quad A = O(p^{-1}(\log p)^4) \quad \text{as } p \rightarrow \infty.$$

Using symmetry of $\Omega(\kappa, \lambda, \mu)$ and $\Gamma(k, \ell, m)$ with respect to interchanging their arguments, the sum B can be written as

$$B = \frac{4}{p^6} \Omega(0, 0, 0) \Gamma(0, 0, 0) + \frac{4}{p^6} \sum_{k=1}^{p-1} \Omega(k\beta, k\beta, 0) \Gamma(k, k, 0) (2\epsilon_k + \epsilon_k^{2S}).$$

Application of (21) and (25) to evaluate $\Omega(k\beta, k\beta, 0)$ and $\Gamma(k, k, 0)$ then gives

$$(32) \quad B = \frac{(p^2 + 2)(p^2 - 1)}{12p^4} + \frac{2(p^2 - 2)}{p^4} \sum_{k=1}^{p-1} \frac{2 + \epsilon_k^{2S-1}}{|1 - \epsilon_k|^2}.$$

We wish to apply the identity

$$(33) \quad \sum_{k=1}^{p-1} \frac{\epsilon_k^j}{|1 - \epsilon_k|^2} = \frac{p^2}{2} \left(\frac{|j|}{p} - \frac{1}{2} \right)^2 - \frac{p^2 + 2}{24} \quad \text{for integer } j \text{ satisfying } |j| \leq p$$

(see [15, p. 621], for example). Since $\frac{1}{2} < s \leq \frac{1}{2}$, we have $|2S - 1| \leq p$ for all sufficiently large p , which allows us to apply (33) to (32) to obtain, for all sufficiently large p ,

$$B = \frac{(p^2 + 2)(p^2 - 1)}{12p^4} + \frac{(p^2 - 2)^2}{4p^4} + \frac{p^2 - 2}{p^2} \left(\frac{|2S - 1|}{p} - \frac{1}{2} \right)^2.$$

By the definition of S , we have $S = ps + O(1)$ as $p \rightarrow \infty$, and therefore,

$$(34) \quad B = \frac{1}{3} + 4 \left(|s| - \frac{1}{4} \right)^2 + O(p^{-1}) \quad \text{as } p \rightarrow \infty.$$

The proof is completed by substituting (31) and (34) in (30). \square

Lemma 5.6. *Let Z be a ternary quadratic-residue array of size $p \times p$, and let s and t be real numbers satisfying $-\frac{1}{2} < s, t \leq \frac{1}{2}$. Then, as $p \rightarrow \infty$,*

$$\frac{1}{4p^6} \sum_{0 \leq i, j < p} |Z_{s,t}(-\epsilon_i, -\epsilon_j)|^4 = \frac{4}{9} + 64(|s| - \frac{1}{4})^2(|t| - \frac{1}{4})^2 + O(p^{-1}(\log p)^8).$$

Proof. The idea of the proof is similar to that of the proof of Lemma 5.5. The main difference is that we now have to apply interpolation of $Z_{s,t}(x, y)$ in both indeterminates.

Let i and j be integer. By the interpolation formula (28) we have

$$Z_{s,t}(-\epsilon_i, -\epsilon_j) = \frac{2}{p} \sum_{k=0}^{p-1} Z_{s,t}(\epsilon_k, -\epsilon_j) \frac{\epsilon_k}{\epsilon_k + \epsilon_i}.$$

Apply the interpolation formula (28) again to obtain

$$Z_{s,t}(-\epsilon_i, -\epsilon_j) = \frac{4}{p^2} \sum_{0 \leq k, \ell < p} Z_{s,t}(\epsilon_k, \epsilon_\ell) \frac{\epsilon_k}{\epsilon_k + \epsilon_i} \frac{\epsilon_\ell}{\epsilon_\ell + \epsilon_j}.$$

Set $S := \lfloor ps \rfloor$ and $T := \lfloor pt \rfloor$. Then by (27) and Lemma 5.1 we get

$$Z_{s,t}(-\epsilon_i, -\epsilon_j) = \frac{4}{p} (-1)^{\frac{p+1}{2}} \sum_{0 \leq k, \ell < p} \epsilon_k^{-S} \epsilon_\ell^{-T} \chi(k\beta + \ell\beta') \frac{\epsilon_k}{\epsilon_k + \epsilon_i} \frac{\epsilon_\ell}{\epsilon_\ell + \epsilon_j},$$

where χ is the quadratic character of $\text{GF}(p^2)$ and $\{\beta, \beta'\}$ is some basis for $\text{GF}(p^2)$ over $\text{GF}(p)$. Since we also have

$$\overline{Z_{s,t}(-\epsilon_i, -\epsilon_j)} = \frac{4}{p} (-1)^{\frac{p+1}{2}} \sum_{0 \leq k, \ell < p} \epsilon_k^S \epsilon_\ell^T \chi(k\beta + \ell\beta') \frac{\epsilon_i}{\epsilon_k + \epsilon_i} \frac{\epsilon_j}{\epsilon_\ell + \epsilon_j},$$

we obtain

$$\begin{aligned} |Z_{s,t}(-\epsilon_i, -\epsilon_j)|^4 &= \left(\frac{4}{p}\right)^4 \sum_{0 \leq a, b, c, d < p} \sum_{0 \leq a', b', c', d' < p} \epsilon_{b-a+d-c}^S \epsilon_{b'-a'+d'-c'}^T \\ &\quad \chi(a\beta + a'\beta') \chi(b\beta + b'\beta') \chi(c\beta + c'\beta') \chi(d\beta + d'\beta') \\ &\quad \frac{\epsilon_a}{\epsilon_a + \epsilon_i} \frac{\epsilon_{a'}}{\epsilon_{a'} + \epsilon_j} \frac{\epsilon_b}{\epsilon_b + \epsilon_i} \frac{\epsilon_{b'}}{\epsilon_{b'} + \epsilon_j} \frac{\epsilon_c}{\epsilon_c + \epsilon_i} \frac{\epsilon_{c'}}{\epsilon_{c'} + \epsilon_j} \frac{\epsilon_d}{\epsilon_d + \epsilon_i} \frac{\epsilon_{d'}}{\epsilon_{d'} + \epsilon_j}. \end{aligned}$$

Use (29), relabel the summation indices, and use the definition (19) of $\Omega(\kappa, \lambda, \mu)$ to give

$$\begin{aligned} \sum_{0 \leq i, j < p} |Z_{s,t}(-\epsilon_i, -\epsilon_j)|^4 &= \frac{256}{p^4} \sum_{0 \leq k, \ell, m < p} \sum_{0 \leq k', \ell', m' < p} \epsilon_{k-\ell+m}^S \epsilon_{k'-\ell'+m'}^T \epsilon_\ell \epsilon_{\ell'} \\ &\quad \Omega(k\beta + k'\beta', \ell\beta + \ell'\beta', m\beta + m'\beta') \Gamma(k, \ell, m) \Gamma(k', \ell', m'). \end{aligned}$$

Let I be the set defined in (20), and write

$$(35) \quad \frac{1}{4p^6} \sum_{0 \leq i, j < p} |Z_{s,t}(-\epsilon_i, -\epsilon_j)|^4 = A + B,$$

where

$$\begin{aligned}
A &= \frac{64}{p^{10}} \sum_{\substack{0 \leq k, \ell, m, k', \ell', m' < p \\ (k\beta + k'\beta', \ell\beta + \ell'\beta', m\beta + m'\beta') \notin I}} \epsilon_{k-\ell+m}^S \epsilon_{k'-\ell'+m'}^T \epsilon_\ell \epsilon_{\ell'} \\
&\quad \Omega(k\beta + k'\beta', \ell\beta + \ell'\beta', m\beta + m'\beta') \Gamma(k, \ell, m) \Gamma(k', \ell', m') \\
B &= \frac{64}{p^{10}} \sum_{\substack{0 \leq k, \ell, m, k', \ell', m' < p \\ (k\beta + k'\beta', \ell\beta + \ell'\beta', m\beta + m'\beta') \in I}} \epsilon_{k-\ell+m}^S \epsilon_{k'-\ell'+m'}^T \epsilon_\ell \epsilon_{\ell'} \\
&\quad \Omega(k\beta + k'\beta', \ell\beta + \ell'\beta', m\beta + m'\beta') \Gamma(k, \ell, m) \Gamma(k', \ell', m').
\end{aligned}$$

From (22) we have the bound

$$\begin{aligned}
|A| &\leq \frac{192}{p^9} \left(\sum_{0 \leq k, \ell, m < p} |\Gamma(k, \ell, m)| \right)^2 \\
&\leq 192 p^{-1} (\log p)^8
\end{aligned}$$

by (26), giving

$$(36) \quad A = O(p^{-1} (\log p)^8) \quad \text{as } p \rightarrow \infty.$$

We use symmetry of $\Omega(\kappa, \lambda, \mu)$ and $\Gamma(k, \ell, m)$ with respect to interchanging their arguments to partition the sum B further as

$$(37) \quad B = B_1 + B_2 + B_3 + B_4,$$

where

$$\begin{aligned}
B_1 &= \frac{64}{p^{10}} \Omega(0, 0, 0) [\Gamma(0, 0, 0)]^2 \\
B_2 &= \frac{64}{p^{10}} \sum_{k=1}^{p-1} \Omega(k\beta, k\beta, 0) \Gamma(k, k, 0) \Gamma(0, 0, 0) (2\epsilon_k + \epsilon_k^{2S}) \\
B_3 &= \frac{64}{p^{10}} \sum_{k'=1}^{p-1} \Omega(k'\beta', k'\beta', 0) \Gamma(0, 0, 0) \Gamma(k', k', 0) (2\epsilon_{k'} + \epsilon_{k'}^{2T}) \\
B_4 &= \frac{64}{p^{10}} \sum_{1 \leq k, k' < p} \Omega(k\beta + k'\beta', k\beta + k'\beta', 0) \Gamma(k, k, 0) \Gamma(k', k', 0) (2\epsilon_k \epsilon_{k'} + \epsilon_k^{2S} \epsilon_{k'}^{2T}).
\end{aligned}$$

Application of (21) and (25) to evaluate $\Omega(\kappa, \kappa, 0)$ and $\Gamma(k, k, 0)$ then gives

$$\begin{aligned}
B_1 &= \frac{1}{36} \frac{(p^2 + 2)^2 (p^2 - 1)}{p^6} \\
B_2 &= \frac{2}{3} \frac{p^4 - 4}{p^6} \sum_{k=1}^{p-1} \frac{2 + \epsilon_k^{2S-1}}{|1 - \epsilon_k|^2} \\
B_3 &= \frac{2}{3} \frac{p^4 - 4}{p^6} \sum_{k=1}^{p-1} \frac{2 + \epsilon_k^{2T-1}}{|1 - \epsilon_k|^2} \\
B_4 &= 16 \frac{p^2 - 2}{p^6} \sum_{1 \leq k, k' < p} \frac{2 + \epsilon_k^{2S-1} \epsilon_{k'}^{2T-1}}{|1 - \epsilon_k|^2 |1 - \epsilon_{k'}|^2}.
\end{aligned}$$

We complete the proof by evaluating the asymptotic behavior of the terms B_1 , B_2 , B_3 , and B_4 .

The term B_1 : The term B_1 becomes

$$(38) \quad B_1 = \frac{1}{36} + O(p^{-2}) \quad \text{as } p \rightarrow \infty.$$

The terms B_2 and B_3 : Since $-\frac{1}{2} < s \leq \frac{1}{2}$ implies that $|2S - 1| \leq p$ for all sufficiently large p , we can use the identity (33) to write

$$B_2 = \frac{2}{3} \frac{p^4 - 4}{p^6} \left[\frac{p^2 - 2}{8} + \frac{p^2}{2} \left(\frac{|2S - 1|}{p} - \frac{1}{2} \right)^2 \right].$$

Then, since $S = ps + O(1)$ as $p \rightarrow \infty$, we obtain

$$(39) \quad B_2 = \frac{1}{12} + \frac{4}{3}(|s| - \frac{1}{4})^2 + O(p^{-1}) \quad \text{as } p \rightarrow \infty.$$

We proceed similarly for the term B_3 and find that

$$(40) \quad B_3 = \frac{1}{12} + \frac{4}{3}(|t| - \frac{1}{4})^2 + O(p^{-1}) \quad \text{as } p \rightarrow \infty.$$

The term B_4 : The term B_4 can be rewritten as

$$B_4 = 16 \frac{p^2 - 2}{p^6} \left[2 \left(\sum_{k=1}^{p-1} \frac{1}{|1 - \epsilon_k|^2} \right)^2 + \left(\sum_{k=1}^{p-1} \frac{\epsilon_k^{2S-1}}{|1 - \epsilon_k|^2} \right) \left(\sum_{k'=1}^{p-1} \frac{\epsilon_{k'}^{2T-1}}{|1 - \epsilon_{k'}|^2} \right) \right].$$

Noting that $|2S - 1| \leq p$ and $|2T - 1| \leq p$ for all sufficiently large p , application of (33) gives

$$B_4 = \frac{2}{9} \frac{(p^2 - 2)(p^2 - 1)^2}{p^6} + 16 \frac{p^2 - 2}{p^6} \left[\frac{p^2}{2} \left(\frac{|2S - 1|}{p} - \frac{1}{2} \right)^2 - \frac{p^2 + 2}{24} \right] \left[\frac{p^2}{2} \left(\frac{|2T - 1|}{p} - \frac{1}{2} \right)^2 - \frac{p^2 + 2}{24} \right].$$

Since $S = ps + O(1)$ and $T = pt + O(1)$ as $p \rightarrow \infty$, we finally obtain

$$(41) \quad B_4 = \frac{2}{9} + \left[8(|s| - \frac{1}{4})^2 - \frac{1}{6} \right] \left[8(|t| - \frac{1}{4})^2 - \frac{1}{6} \right] + O(p^{-1}) \quad \text{as } p \rightarrow \infty.$$

The result now follows by substituting the asymptotic forms (38), (39), (40), and (41) into (37) and then (37) and (36) into (35). \square

We are now able to prove the main result of this section.

Theorem 5.7. *Let Y be a quadratic-residue array of size $p \times p$, and let s and t be real numbers satisfying $-\frac{1}{2} < s, t \leq \frac{1}{2}$. Then*

$$\lim_{p \rightarrow \infty} \frac{1}{F(Y_{s,t})} = \frac{1}{9} + \left[\frac{1}{2} + 8 \left(|s| - \frac{1}{4} \right)^2 \right] \left[\frac{1}{2} + 8 \left(|t| - \frac{1}{4} \right)^2 \right].$$

Proof. Let Z be a ternary quadratic-residue array of size $p \times p$. From (16) we have

$$\begin{aligned} \frac{1}{p^4} \sum_{u,v} [C_{Z_{s,t}}(u,v)]^2 &= \frac{1}{4p^6} \sum_{0 \leq i,j < p} |Z_{s,t}(\epsilon_i, \epsilon_j)|^4 + \frac{1}{4p^6} \sum_{0 \leq i,j < p} |Z_{s,t}(-\epsilon_i, \epsilon_j)|^4 \\ &\quad + \frac{1}{4p^6} \sum_{0 \leq i,j < p} |Z_{s,t}(\epsilon_i, -\epsilon_j)|^4 + \frac{1}{4p^6} \sum_{0 \leq i,j < p} |Z_{s,t}(-\epsilon_i, -\epsilon_j)|^4. \end{aligned}$$

Using Lemmas 5.4, 5.5, and 5.6 to determine the asymptotic behavior of the sums on the right-hand side, we obtain

$$(42) \quad \frac{1}{p^4} \sum_{u,v} [C_{Z_{s,t}}(u,v)]^2 = \frac{10}{9} + \left[\frac{1}{2} + 8 \left(|s| - \frac{1}{4} \right)^2 \right] \left[\frac{1}{2} + 8 \left(|t| - \frac{1}{4} \right)^2 \right] + O(p^{-1}(\log p)^8) \quad \text{as } p \rightarrow \infty.$$

Now, since the binary array Y differs from the ternary array Z only in a single position, we have

$$C_{Y_{s,t}}(u,v) = C_{Z_{s,t}}(u,v) + \delta(u,v),$$

where

$$(43) \quad |\delta(u,v)| \leq \begin{cases} 1 & \text{for } -p < u, v < p \\ 0 & \text{otherwise.} \end{cases}$$

Then, by the Cauchy-Schwarz inequality,

$$\begin{aligned} & \left| \sum_{u,v} [C_{Y_{s,t}}(u,v)]^2 - \sum_{u,v} [C_{Z_{s,t}}(u,v)]^2 \right| \\ & \leq \sum_{u,v} [\delta(u,v)]^2 + 2 \left(\sum_{u,v} [C_{Z_{s,t}}(u,v)]^2 \right)^{1/2} \left(\sum_{u,v} [\delta(u,v)]^2 \right)^{1/2}, \end{aligned}$$

so that by (43) and (42)

$$\frac{1}{p^4} \left| \sum_{u,v} [C_{Y_{s,t}}(u,v)]^2 - \sum_{u,v} [C_{Z_{s,t}}(u,v)]^2 \right| = O(p^{-1}) \quad \text{as } p \rightarrow \infty.$$

The theorem follows from (42) by noting that $C_{Y_{s,t}}(0,0) = p^2$. \square

6. CONCLUDING REMARKS

We have computed the asymptotic value of the merit factor of Legendre arrays (under certain conditions on the growth rate of their dimensions) and of quadratic-residue arrays, for all rotations of rows and columns. The asymptotic merit factor of rotated Legendre arrays and rotated quadratic-residue arrays is shown in Figures 1 and 2, respectively. The maximum asymptotic merit factor, taken over all rotations, equals $\frac{36}{13} \simeq 2.77$ for both array families, which occurs at the rotations (s,t) , where $s, t \in \{\frac{1}{4}, \frac{3}{4}\}$. However, at all other rotations, the asymptotic merit factor of quadratic-residue arrays is larger than that of Legendre arrays. On the other hand, an advantage of Legendre arrays is that they are not restricted to be square.

In [4], the authors exhibited a family of sequences A obtained by appending an initial fraction of a rotated Legendre sequence to itself. Based on partial explanations and extensive numerical computations, it was conjectured in [4] that this sequence family has asymptotic merit factor greater than 6.34. Under the assumption that this conjecture is correct, the corresponding square product array $A \times A$ has asymptotic merit factor greater than 2.93, by (3). This suggests that the maximum asymptotic value of the merit factor of the two array families considered in this paper, namely $\frac{36}{13} \simeq 2.77$, can be surpassed by another array family.

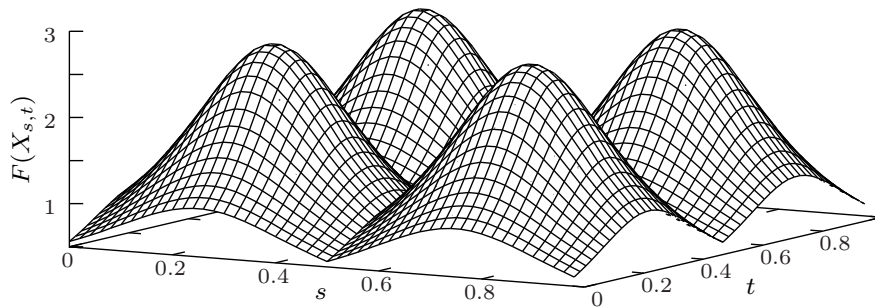


FIGURE 1. The asymptotic value of $F(X_{s,t})$ (under conditions specified in Theorem 4.3), where X is a Legendre array.

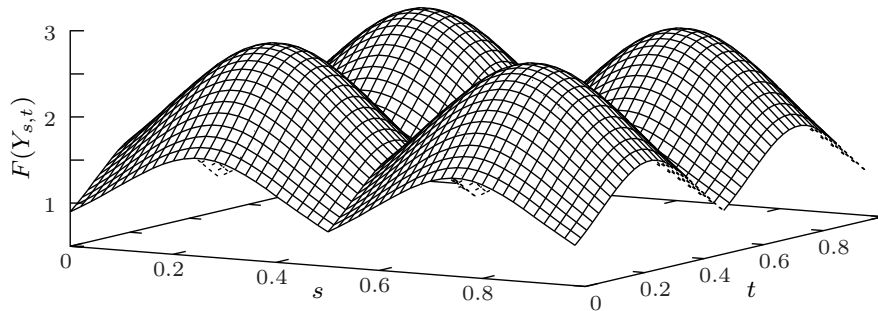


FIGURE 2. The asymptotic value of $F(Y_{s,t})$, where Y is a quadratic-residue array.

In closing, we remark that instead of studying the merit factor of two-dimensional arrays of size $n \times m$, Gulliver and Parker [8] studied the (suitably generalised) merit factor of d -dimensional arrays of size $2 \times 2 \times \cdots \times 2$. In [8], the merit factor of several families of such arrays was calculated. In particular, the largest asymptotic value, as $d \rightarrow \infty$, of the merit factor of a family of d -dimensional arrays considered in [8] equals 3.

ACKNOWLEDGEMENTS

I would like to thank Jonathan Jedwab for valuable discussions on the subject and for careful comments on a draft of this paper.

REFERENCES

- [1] S. Alquaddoomi and R. A. Scholtz, *On the nonexistence of Barker arrays and related matters*, IEEE Trans. Inf. Theory **35** (1989), 1048–1057.
- [2] L. Bömer and M. Antweiler, *Optimizing the aperiodic merit factor of binary arrays*, Signal Process. **30** (1993), 1–13.
- [3] L. Bömer, M. Antweiler, and H. Schotten, *Quadratic residue arrays*, Frequenz **47** (1993), 190–196.
- [4] P. Borwein, K.-K. S. Choi, and J. Jedwab, *Binary sequences with merit factor greater than 6.34*, IEEE Trans. Inf. Theory **50** (2004), 3234–3249.
- [5] D. Calabro and J. K. Wolf, *On the synthesis of two-dimensional arrays with desirable correlation properties*, Inform. Control **11** (1967), 537–560.

- [6] J. A. Davis, J. Jedwab, and K. W. Smith, *Proof of the Barker array conjecture*, Proc. Amer. Math. Soc. **135** (2007), 2011–2018.
- [7] H. Eggers, “Synthese zweidimensionaler Folgen mit guten Autokorrelationseigenschaften,” Ph.D. thesis, RWTH Aachen, Germany, 1986.
- [8] T. A. Gulliver and M. G. Parker, *The multivariate merit factor of a Boolean function*, in “Coding and Complexity” (ed. M. J. Dinneen), IEEE, (2005), 58–62.
- [9] T. Høholdt and H. E. Jensen, *Determination of the merit factor of Legendre sequences*, IEEE Trans. Inf. Theory **34** (1988), 161–164.
- [10] T. Høholdt, H. E. Jensen, and J. Justesen, *Aperiodic correlations and the merit factor of a class of binary sequences*, IEEE Trans. Inf. Theory **IT-31** (1985), 549–552.
- [11] J. Jedwab, *A survey of the merit factor problem for binary sequences*, in “Sequences and Their Applications,” (eds. T. Helleseth et al.), Lecture Notes in Computer Science, vol. 3486, Springer Verlag, (2005), 30–55.
- [12] J. Jedwab and K.-U. Schmidt, *The merit factor of binary sequence families constructed from m -sequences*, Contemp. Math. **518** (2010), 265–278.
- [13] J. Jedwab and K.-U. Schmidt, *The L_4 norm of Littlewood polynomials derived from the Jacobi symbol*, submitted for publication (2010).
- [14] H. E. Jensen and T. Høholdt, *Binary sequences with good correlation properties*, in “Applied Algebra, Algebraic Algorithms and Error-Correcting Codes”, (eds. L. Huguët and A. Poli), Lecture Notes in Computer Science, vol. 356, Springer-Verlag, (1989), 306–320.
- [15] J. M. Jensen, H. E. Jensen, and T. Høholdt, *The merit factor of binary sequences related to difference sets*, IEEE Trans. Inf. Theory **37** (1991), 617–626.
- [16] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, 1997.
- [17] J. E. Littlewood, *Some Problems In Real And Complex Analysis*, Heath Mathematical Monographs, D. C. Heath and Company, Lexington, MA, 1968.
- [18] M. J. Mossinghoff, *Wieferich pairs and Barker sequences*, Des. Codes Cryptogr. **53** (2009), 149–163.
- [19] D. V. Sarwate, *Mean-square correlation of shift-register sequences*, IEE Proc. **131**, Part F (1984), 101–106.
- [20] K.-U. Schmidt, J. Jedwab, and M. G. Parker, *Two binary sequence families with large merit factor*, Adv. Math. Commun. **3** (2009), 135–156.
- [21] M. R. Schroeder, *Number Theory In Science and Communication: With Applications In Cryptography, Physics, Digital Information, Computing, And Self-similarity*, 3rd ed., Springer, Berlin, 1997.
- [22] R. Turyn and J. Storer, *On binary sequences*, Proc. Amer. Math. Soc. **12** (1961), 394–399.
- [23] R. G. van Schyndel, A. Z. Tirkel, I. D. Svalbe, T. E. Hall, and C. F. Osborne, *Algebraic construction of a new class of quasi-orthogonal arrays for steganography*, Proceedings of SPIE **3657** (1999), 354–364.

DEPARTMENT OF MATHEMATICS, SIMON FRASER UNIVERSITY, 8888 UNIVERSITY DRIVE, BURNABY BC V5A 1S6, CANADA.

E-mail address: kuschmidt@sfu.ca